NORTH DAKOTA

HOMELAND SECURITY

ANTI-TERRORISM SUMMARY

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

QUICK LINKS

North Dakota

Nothing Significant to Report

Regional

(Minnesota) **Duluth norovirus outbreak linked to ill food-service employee.** A food worker was the most likely source of the illness that sickened at least 60 people who ate at the Greysolon Plaza Ballroom in Duluth, Minnesota, December 3, the Minnesota Department of Health (MDH) confirmed January 4. That coincided with the preliminary conclusion the MDH reached a week after the incident. "Multiple ill employees were identified, indicating the contamination of ready-to-eat food by an ill food worker was the most likely source of contamination," said a MDH spokesman. The department confirmed the culprit was norovirus, the most common food-related illness in Minnesota. It is often spread by food handlers who do not thoroughly wash their hands. About 250 people attended one event and 100 attended another at the Greysolon December 3, state officials said. Source: http://www.duluthnewstribune.com/event/article/id/219044/

(Minnesota) **Busted pipe cited in 500-gallon bleach leak at Xcel nuke plant.** Five hundred gallons of chlorine bleach leaked from a tank January 5 at the Prairie Island nuclear plant near Red Wing, Minnesota, prompting an emergency response from Xcel Energy and delaying classes in two nearby school districts. The leak of sodium hypochloride was discovered by a worker. Xcel said the leak is fully contained within a berm, and a clean-up crew was cleaning up the site January 5. The leak led to the utility declaring an alert, which is the second lowest of four emergency classifications established by the Nuclear Regulatory Commission. As a precaution, schools in the Prescott and Ellsworth districts in Wisconsin delayed the start of classes for 2 hours. Source: http://www.startribune.com/local/136729298.html

(Montana) **Wildfires at Montana Indian Reservation force evacuations.** Two wildfires raging January 4 on Montana's Blackfeet Indian Reservation burned thousands of acres, forced hundreds to evacuate, and destroyed several buildings, officials said January 5. Fueled by strong winds, the two fires started and together had grown to at least 45,000 acres. At least 300 people were forced to leave their homes, and officers were working to evacuate additional residents in the fires' eastward path. One fire started southeast of Browning burned about 8 miles east to the community of Blackfoot, a tribal spokesman said. Another fire erupted around the same time about 10 miles away. The Blackfeet Law Enforcement chief told the Great Falls Tribune the fires were started by what was believed to be power lines that were blown over by high winds. One fire that burned east of Browning had already been put out. Source: http://www.firehouse.com/news/10603872/wildfires-at-montana-indian-reservation-force-evacuations

(Montana) **A long road of flood repairs still ahead for Montana.** The 2011 floods are in Montana's past, but repairing the damage to roads is proving to be long, jarring, and costly. The state department of transportation lists $41.3 million in repairs on the roads it is responsible

for, with much work still to be done. The projects number more than 100 and do not include road repairs on county roads, where the burden of the bill falls on local governments. The state was quick to get roads reopened, but repairs will continue for some time, said the chief of the department's planning, policy, and analysis bureau. In central Montana, where hillsides heavy with water sloughed away, taking half a road with them, solar-powered traffic lights in the middle of nowhere became a common sight, as the transportation department rushed to keep oncoming cars from crowding what little road remained. In Fergus County, the number of weather-affected road areas at one point numbered 139 and included everything from washed-out culverts and landslides to chewed-up pavement and damaged bridges. The cost is expected to be $10 million, or more than six times what the county spends on roads in an average year. Fergus County still has nine bridges needing repairs. Through August 2011, Montana received $24 million from Federal Emergency Management Agency (FEMA) for public infrastructure repairs, though the final deadline for a FEMA request was not until October 11. FEMA approved more $50 million for Montana public assistance requests related to infrastructure. Source: http://billingsgazette.com/news/state-and-regional/montana/a-long-road-of-flood-repairs-still-ahead-for-montana/article_735f1d07-dc9e-5dcb-9530-f88aa885c8a5.html#ixzz1iatUpW00

(South Dakota) **Gavins Point spillway likely to remain open through February.** The U. S. Army Corps of Engineers announced that releases will likely continue through the spillway at the Gavins Point Project in South Dakota through the end of February, KCAU 9 Sioux City reported January 4. Releases are expected to be around 22,000 cubic feet per second (cfs) to help gain additional reservoir system storage in preparation for the 2012 runoff season. As water continues to be released through the spillway, hazardous conditions exist for any vessel in the area,and boaters are urged to use caution. Source: http://www.kcautv.com/story/16446526/spillway-likely-to-remain-open-through-february

National

Smart grid security inadequate, threats abound. A recent report by Pike Research found a lack of security standards, ahodgepodge of products, and increasingly aggressive malicious hackers will make 201a challenging year for securing smart grids, IDG News Service reported January 4. "After years of vendors selling point solutions, utilities investing in compliance minimums rather than full security, and attackers having nearly free rein, the attackers clearly have the upper hand. Many attacks simply cannot be defended," said a Pike 2 analyst. There is also a danger of overlooking the insider threat. "One of the main reasons for increased spending on smart grid security software and management systems is simply to make sure the correct people have access to the equipment and systems they should have access to." Among other things, this means protecting systems from disgruntled employees or others who might commit internal sabotage, an ABI Research analyst said. The Pike Research report suggests the lack of enforceable security standards or regulations for power distribution grids "leads to a scene of mass chaos in utility cybersecurity", and will cause utilities to take a wait-and-see approach to significant security investments. Source: http://news.idg.no/cw/art.cfm?id=A127ABC9-B53E-AC90-3176B393E1D42341

EPA cross-state emissions rule put on hold by appeals court. The U.S. Environmental Protection Agency (EPA) must delay implementing rules on interstate air pollution January 1, a federal court ruled December 30, siding with electric power producers seeking to defeat them. A three-judge appellate court panel granted a request by electric power producers and other challengers to delay the deadline for plants in 27 states to begin reducing emissions of sulfur dioxide and nitrogen oxide while the court considers the rule's legality. More than three dozen lawsuits seek to derail the Cross-State Air Pollution Rule, which was issued in July and revised in October. The court has not scheduled a date for argument, though the order suggested the judges would hear the case by April. Southern Co., EME Homer City Generation LP, a unit of Edison International, and Energy Future Holdings Corp. units in Texas are among the power companies challenging the rule. The state of Texas, the National Mining Association and the International Brotherhood of Electrical Workers joined in parallel cases, saying the rule puts an undue financial burden on power producers and threatens electricity reliability by forcing companies to shut some older plants. Source: http://www.businessweek.com/news/2012-01-03/epa-cross-state-emissions-rule-put-on-hold-by-appeals-court.html

International

Vancouver police probing L.A. arson suspect over unsolved fires. The investigation of an Los Angeles-area arson suspect widened January 5 to include a probe by Canadian authorities into whether he was involved in a series of suspicious fires in Vancouver, Canada. The suspect who has been charged with 37 felony counts related to the New Year's weekend arson rampage, lived in Vancouver with his mother before moving to the Los Angeles area. A Vancouver Police Department spokeswoman said officials "have begun to liaise with the LAPD" but stressed detectives have not connected the suspect to any specific fires in that city. News of the probe comes a day after German prosecutors confirmed the suspect was also under investigation for suspected arson and insurance fraud in the October 14, 2011, fire that caused major damage to a half-timbered duplex in the mountainous region near Marburg in central Germany. U.S. immigration officials have confirmed the suspect flew from Frankfurt to Las Vegas 6 days after the fire. Authorities said the suspect was "motivated by his rage against Americans" when he allegedly set the fires in Los Angeles. The fires began after his mother was detained by authorities on a German criminal warrant. Source: http://latimesblogs.latimes.com/lanow/2012/01/vancouver-police-probing-la-arson-suspect.html

Banking and Finance Industry

SpyEye malware borrows Zeus trick to mask fraud. A powerful bank-fraud software program, SpyEye, has been seen with a feature designed to keep victims in the dark long after fraud has taken place, according to a January 4 report from security vendor Trusteer. SpyEye is notable for its ability to inject new fields into a Web page, a technique called HTML injection, which can ask banking customers for sensitive information they normally would not be asked. The requested data can include logins and passwords or a debit card number. It can also use HTML injection to hide fraudulent transfers of money out of an account by displaying an inaccurate

bank balance. Trusteer found SpyEye also hides fraudulent transactions even after a person has logged out and logged back into their account. SpyEye does this by checking its records to see what fraudulent transactions were made with the account, then deleting them from the Web page, said Trusteer's chief executive officer (CEO). The account balance is also altered. It appears SpyEye has borrowed from Zeus, a famous piece of banking malware now commonly available and considered its parent. Trusteer has seen the technique used when a fraudster uses SpyEye to capture debit card details. When that data is obtained, the fraudster conducts a purchase over the Web or phone, and SpyEye masks the transaction, the CEO said. It does not affect, however, the bank's ability to see the fraud, he said. Source: http://www.pcworld.com/businesscenter/article/247252/spyeye_malware_borrows_zeus_trick_to_mask_fraud.html

US charges Swiss bankers for hiding $1.2 billion. Three Swiss bankers were indicted in the United States January 3, accused of hiding $1.2 billion in assets of U.S. clients seeking to avoid declaring their full wealth to tax authorities. The bankers were accused of "conspiring with U.S. taxpayers and others" in a massive tax fraud scheme. In an indictment, the bankers were said to have been client advisers at the Zurich branch of an institution identified as "Swiss Bank A." They allegedly conspired with U.S. clients to hide the existence of bank accounts and the income they generated from the Internal Revenue Service. Swiss banks, which have a longstanding practice of offering clients secrecy, have come under steady attack by U.S. authorities, highlighted by a probe into banking giant UBS which led to a deal between U.S. and Swiss authorities. The service by "Bank A" was allegedly ramped up in 2008 and 2009 "ito capture business lost by UBS AG and another large international Swiss bank in the wake of widespread news reports that the IRS was investigating UBS for helping U.S. taxpayers evade taxes and hide assets in Swiss bank accounts," New York federal prosecutors said in a statement. They "allegedly told various U.S. taxpayer-clients that their undeclared accounts at Swiss Bank A would not be disclosed to the United States authorities because Swiss Bank A had a long tradition of bank secrecy." The three bankers live in Switzerland. If convicted in the United States they would each face a maximum term of 5 years in prison. Source: http://www.google.com/hostednews/afp/article/ALeqM5joM8NiVLMsAOLv2EeeDxDwOpDPzg?docId=CNG.5d4866e77b6f7d7b4a432c8d01267956.741

Financial services firm pleads guilty to municipal bond fraud. Beverly Hills, California-based Rubin/Chambers, Dunhill Insurance Services (also known as CDR Financial Products), and its founder and owner pleaded guilty December 30 to bid-rigging and fraud conspiracies involving investment of municipal bond proceeds and other related municipal finance contracts. CDR and its founder pleaded guilty to participating in separate bid-rigging and fraud conspiracies with various financial institutions and insurance companies and their representatives. They offered a type of contract, known as an investment agreement, to state, county, and local governments and agencies across the country. CDR was hired to act as a broker and conduct a supposed competitive bidding process for contracts for investing municipal bond proceeds. The firm's founder admitted that, from 1998 until 2006, he and other co-conspirators supplied information to providers to help them win bids, solicited intentionally losing bids, and signed certifications that contained false statements regarding whether the bidding process for certain

investment agreements complied with relevant Treasury Regulations, the announcement said. He also admitted he and other co-conspirators solicited fees from providers, which were in fact payments to CDR for rigging or manipulating bids for certain investment agreements so a particular provider would win that agreement at an artificially determined price. Source: http://www.legalnewsline.com/news/234784-financial-services-firm-pleads-guilty-to-municipal-bond-fraud

Chemical and Hazardous Materials Sector

NRC to review regulations for reactors. The Nuclear Regulatory Commission (NRC) has agreed with environmentalists to review its regulations concerning General Electric Mark 1 reactors. An NRC safety panel posted notice on its Federal Register Web site January 3 accepting a request by three environmental groups to review whether approvals issued in 1989 concerning reactor venting systems at General Electric Mark I reactors should be revoked. The reactor is the same type that was in operation at the Fukushima, Japan nuclear power plant which suffered a meltdown and fire last March. According to a release issued by the environmental groups, the NRC review will also include whether to order all Mark I operators to install backup emergency power systems to cool the reactors' highly radioactive rooftop fuel pools. Source: http://www.courierpostonline.com/article/20120106/NEWS01/301060037/NRC-review-regulations-reactors-Oyster-Creek

EPA: Toxic chemical releases rise 16% in 2010. Reversing a downward trend, the amount of toxic chemicals released into the nation's environment in 2010 was 16 percent higher than the year before, the U.S. Environmental Protection Agency (EPA) reported. Due largely to changes in metal mining, 3.93 billion pounds of toxic chemicals were released into the environment in 2010, according to the EPA's annual Toxics Release Inventory. Such amounts had previously been falling since 2006. "In this sector, even a small change in the chemical composition of ore being mined .... may lead to big changes in the amount of toxic chemicals reported nationally," the EPA said in a statement January 5 accompanying the data release. The agency said the chemical and primary metals industries also reported increases in toxic releases. The problem was most severe with toxic chemical releases into the ground, which jumped 28 percent in 2010. Such releases into surface water rose 9 percent. Total air releases fell 6 percent in 2010, continuing a multi-year downward trend, but those of dioxin rose 10 percent. The EPA is expected this month to release the first part of an environmental assessment of dioxin, which is linked to cancer and neurological problems. Source: http://content.usatoday.com/communities/greenhouse/post/2012/01/epa-toxic-chemical-releases-jump-16-in-2010/1

(New Jersey) **Nuclear plants investigated.** Federal regulators are investigating undisclosed security failings at PSEG Nuclear's big Salem/Hope Creek reactor site in Lower Alloways Township, New Jersey, and warned of possible sanctions and additional citations against the company, the New Castle News Journal reported January 4. Nuclear Regulatory Commission (NRC) officials declined to release details of inspection findings leading to the security citation that was relayed to PSEG in mid-December but made public only recently. A letter posted in the

NRC's public library noted that PSEG "promptly implemented compensatory measures for the deficiency" and was back in compliance with NRC rules before the federal inspection ended. The problems are nevertheless "being considered for escalated enforcement action." Source: http://www.delawareonline.com/article/20120104/NEWS08/201040345/Nuclear-plants-investigated?odyssey=tab|topnews|text|Home

COMMERCIAL FACILITIES

(Iowa) **Police arrest Occupy activists at Des Moines hotel.** Des Moines, Iowa police arrested about a dozen Occupy the Caucuses activists who lay on the floor of a downtown hotel lobby after failing to meet with Democratic Party officials January 2. Police were called to the hotel after activists demanded to meet with Democratic officials. The party earlier announced it was setting up a headquarters at the hotel to get their message out during the caucuses. No Democratic officials met with the protesters, prompting them to lie on the floor. Police said they charged about a dozen people with trespassing. Police arrested protesters almost daily for a week at candidate offices and Democratic Party headquarters. Source: http://www.kcautv.com/story/16430768/police-arrest-occupy-activists-at-des-moines-hotel

(New York) **NYPD questioning man in suspected arson attacks on corner store, Islamic cultural center.** New York City's police commissioner said detectives questioned a man in connection with at least four suspected arson attacks that might be bias crimes, the Associated Press reported January 3. He said authorities believe the suspect was kicked out of a store December 22 for trying to steal glass Starbucks bottles. He said four of the five attacks January 1 were done with Molotov cocktails made from such bottles. Police said they found the suspect through video of his car. They are investigating the attacks as possible hate crimes, but it is not clear what group was targeted, if any. The bottles were thrown at an Islamic cultural center, a convenience store, and two homes. One of the homes was used as a Hindu worship site. Source: http://www.washingtonpost.com/national/nyc-police-probe-firebombing-attack-on-prominent-islamic-center-3-other-sites/2012/01/03/gIQAhXNcXP_story.html

(California) **24-year-old arrested in Los Angeles arson spree.** Authorities arrested a German man January 2 in connection with dozens of suspected arson attacks that destroyed parked cars, scorched buildings, and rattled much of Los Angeles over the New Year's weekend. The suspect was booked for investigation of arson of an inhabited dwelling and was being held without bail, authorities said. The suspect is a German national, but authorities said they did not know how long he has been in the United States. Fires were reported in nearly two dozen locations in Hollywood and the neighboring city of West Hollywood during a 4-hour period before dawn December 30. In nearly every case, the fire started in a parked car. Several more cars burned December 31 in the North Hollywood area, and authorities investigated if they were connected. More than 50 blazes had flared since December 30 in Hollywood, neighboring West Hollywood and the San Fernando Valley, causing about $3 million in damage. Firefighters have not responded to any other suspicious fires since the suspect was detained. The fires forced many apartment dwellers from their homes. One of the fires December 31 occurred at the Hollywood and Highland entertainment complex, a popular tourist destination bordered by

the Walk of Fame in a neighborhood that includes Grauman's Chinese Theatre. Hundreds of investigators, police officers, and firefighters raced to deal with the fires. Source: http://www.foxnews.com/us/2012/01/02/la-authorities-respond-to-as-many-as-eight-new-fires-amid-arson-spree/

Communications Sector

(Louisiana) **Ex-AT&T employee accused of stealing copper wire from company sites.** An ex-AT&T employee who had been allegedly stealing spools of copper wire from his former employer for weeks was arrested after being caught inside a storage site near Covington, Louisiana, a spokesman from the St. Tammany Parish Sheriff's Office said January 3. Deputies have booked the man with breaking into the telecommunication firm's facilities on the north shore at least 17 times and pilfering the equipment during 16 of those occasions, an agency spokesman said. Investigators began probing a series of copper thefts from AT&T complexes at the beginning of November, the spokesman said. Many sheriff's divisions subsequently staked out the company's site. On December 28, the suspect was supposedly spotted in the storage yard. He allegedly threw a punch at a deputy who confronted him before he was subdued, the spokesman said. The sheriff's office jailed the suspect in connection with the break-ins, the thefts, and resisting arrest. It expects to add more counts as the investigation develops. Investigators suspect the man was selling the copper to recycling businesses. The suspect worked at AT&T 4 years ago, but no other details of his employment were available. Source: http://www.nola.com/crime/index.ssf/2012/01/ex-att_employee_accused_of_ste.html

Critical Manufacturing

ArcelorMittal hacked by Anonymous, tons of information leaked. Loose-knit hacker collective Anonymous managed to breach the main Web site belonging to ArcelorMittal, the largest steel-producing company in the world, leaking a large quantity of information from their databases, Softpedia reported January 6. ArcelorMittal's Web site was offline January 6. Several cross-site scripting and SQL injection vulnerabilities allowed the hackers to breach the Web site and leak information on users and administrators. Only a few days have passed since Anonymous first threatened Luxembourg-based ArcelorMittal for closing production sites in Belgium. Source: http://news.softpedia.com/news/ArcelorMittal-Hacked-by-Anonymous-Tons-of-Information-Leaked-244898.shtml

Defense/ Industry Base Sector

Aggressive phishing attack targets military. A recent phishing attack is making the rounds in an e-mail which appears be from USAA, a financial services company that serves military members, their families, and veterans, DoD Live reported December 31. The e-mail subject begins with "Deposit Posted." Members are asked to open a Zeus-infected attached file. Once opened, it launches a malicious virus that could provide access to personal information and may require a complete reinstall of the computer operating system. Source: http://www.dodlive.mil/index.php/2011/12/aggressive-phishing-attack-targets-military/

Emergency Services

(Utah) **Utah shooting: 6 police officers shot while serving search warrant.** Gunfire erupted as anti-drug police served a search warrant in an Ogden, Utah neighborhood, fatally wounding one officer and injuring five other officers and a suspect, authorities said. The shots rang out late January 4 as police converged at a residence, a police spokesman said. The six officers were hospitalized along with a suspect. Ogden police said in a statement early January 5 that one agent died from his wounds following the shooting. Five police officers from multiple agencies remain hospitalized with serious to critical injuries. The sole suspect in the shooting is at a local hospital under guard, with non-life threatening injuries. The Ogden Standard-Examiner reported that more police responded upon word of at least one officer shot. The paper said police surrounded the suspect near a backyard shed. The residence was secured after the arrest. Source: http://www.huffingtonpost.com/2012/01/05/utah-shooting-police-officers-wounded_n_1185321.html

(California) **Antisec hacks California Law Enforcement Association, email content leaked.** As part of Project Mayhem, AntiSec hackers took down the official Web site of the California Law Enforcement Association. The site was still down January 3 and the attackers claim other sites hosted on the same domain are also "wiped off the net." Besides defacing the Web site and posting their messages on its main page, the black hats also leaked the contents of some e-mails belonging to their staffers and billing information from customers. The e-mails sent between employees show they suspected they were victim of a data breach, but it took some time for them to change the passwords. Until they did so, the hackers managed to obtain a lot of sensitive data, including the unencrypted content of some database tables that was sent via e-mail. Among one of the e-mails, the hacktivists also found a list of personal e-mail addresses belonging to New York police chiefs. "For our next owning we bring you multiple law enforcement targets in the state of New York, who has been on our crosshairs for some time due to their brutal repression of Occupy Wall Street," they said. Source: http://news.softpedia.com/news/Antisec-Hacks-California-Law-Enforcement-Association-Emails-Content-Leaked-243971.shtml

Energy

(Louisiana) **Study: Loss of Louisiana highway could cripple domestic oil supply.** A DHS study has found temporary disruption of Louisiana Highway LA1 in Lafourche Parish, Louisiana, could potentially cripple the nation's domestic energy supply, as well as cause major damage to the economy, Homeland Security Today reported January 4. The report, titled Louisiana Highway 1/Port Fourchon Study, concluded a 90-day closure of Port Fourchon as a result of a loss of highway access could result in a reduction of up to $7.8 billion in American gross domestic product, while significantly impacting domestic oil and gas production for at least a decade. The DHS's National Infrastructure Simulation and Analysis Center (NISAC) and the National Incident Management Systems and Advanced Technologies (NIMSAT) Institute at University of Louisiana at Lafayette collaborated on the study. Source: http://www.hstoday.us/briefings/today-s-news-

analysis/single-article/study-loss-of-lousiana-highway-could-cripple-domestic-oil-supply/a3720568ca181233129a0a8dea7a3331.html

Expert: Drilling wastewater caused Ohio quakes. A northeast Ohio well used to dispose of wastewater from oil and gas drilling almost certainly caused a series of 11 minor quakes in the Youngstown, Ohio, area since last spring, a seismologist investigating the quakes said January 2. Brine wastewater dumped in wells comes from drilling operations, including the fracking process to extract gas from underground shale that has been a source of concern among environmental groups and some property owners. Injection wells have also been suspected in quakes in Ashtabula in northeast Ohio, and in Arkansas, Colorado, and Oklahoma, said an expert with Columbia University's Lamont-Doherty Earth Observatory in New York. Thousands of gallons of brine were injected daily into the Youngstown well that opened in 2010 until its owner, Northstar Disposal Services LLC, agreed December 30 to stop injecting the waste as a precaution while authorities assessed potential links to the quakes. After the latest and largest 4.0 magnitude quake December 31, state officials announced their belief that injecting wastewater near a fault line had created enough pressure to cause seismic activity. They said four inactive wells within a 5-mile radius of the Youngstown well would remain closed. But they also stressed injection wells are different from drilling wells that employ fracking. One expert believes more quakes will occur despite the shutdown of the Youngstown well. The quakes began last March with the most recent, December 24 and 31, each occurring within 100 meters of the injection well. Source: http://www.cbsnews.com/8301-201_162-57351140/expert-drilling-wastewater-caused-ohio-quakes/

Food and Agriculture

19 ill in drug-resistant Salmonella ground beef outbreak. Nineteen people in seven states have now been confirmed infected with a multi-drug resistant strain of Salmonella Typhimurium in the outbreak linked to contaminated ground beef sold at Hannaford Supermarkets, the Centers for Disease Control and Prevention (CDC) reported January 5. That is three more cases of Salmonella infection confirmed since the CDC's last report on the outbreak, two weeks ago. The new cases were reported in New Hampshire and New York. Hannaford, a chain based in Scarborough, Maine, recalled an undisclosed amount of fresh ground beef December 15. Epidemiologic evidence led outbreak investigators to Hannaford's ground beef. Among 18 of the ill people, 14 recalled eating ground beef the week before they got sick. The outbreak has sent at least seven people to the hospital, the CDC said. They are infected with a strain of Salmonella resistant to several commonly prescribed antibiotics. New Hampshire has reported six cases associated with the outbreak, New York five, and Maine four, while Hawaii, Kentucky, Massachusetts and Vermont each have reported one case. Source: http://www.foodsafetynews.com/2012/01/19-ill-in-drug-resistant-salmonella-ground-beef-outbreak/

Another alert on possible Listeria-contaminated cheese. The Massachusetts Department of Public Health (MDPH) has added a warning to consumers about cheese recalled in November in Canada that may still be in circulation in the United States, Food Safety News reported

December 31. The cheese, linked to one case of listeriosis in Canada, was supplied by Fromagerie Marie Kade of Quebec. The Canadian Food Inspection Agency issued a November 24 health alert notifying residents of Canada of a recall initiated by the dairy plant. This recall followed two previous alerts and extensive product testing, according to Canadian authorities. After a Glendale, California distributor issued a December 26 recall of the cheese distributed in Southern California, the Food and Drug Administration (FDA) notified Massachusetts officials December 28 the product was distributed to Cedar Market in Norwood and that Cedar Market sold the recalled cheese to Bahnan's in Worcester. The MDPH said it worked with the FDA and local officials to embargo and destroy the possibly contaminated cheese and to review inventory records for distribution. Source: http://www.foodsafetynews.com/2011/12/another-alert-on-possible-listeria-contaminated-cheese/

Salmonella sprouts recall expands due to Listeria concerns. A sprouts grower that recalled alfalfa sprouts in December because of a positive Salmonella test is now pulling more varieties off the market because of Listeria concerns, Food Safety News reported January 2. In a news release, Texas-based Green Valley Food Corp. said it is recalling about 35,159 cases of sprouts because several random samples tested positive for Listeria monocytogenes. The recall includes the 650 cases of sprouts recalled December 23 and 24, as well as sprouts that have use-by dates from December 22, 2011 to January 17. The sprouts were distributed in Texas to grocery store distribution centers and food service customers. Source: http://www.foodsafetynews.com/2012/01/sprouts-recall-expands-due-to-listeria-concerns/

Government Sector (including Schools and Universities)

E-voting machine freezes, misreads votes, U.S. agency says. An electronic ballot scanning device slated for use in the upcoming Presidential elections, misreads ballots, fails to log critical events, and is prone to freezes and sudden lockups, the U.S. Elections Assistance Commission (EAC) found. The EAC Formal Investigative Report on the DS200 Precinct Count Optical Scanner in the Unity 3.2.0.0 voting system built by Election Systems & Software was released in late December. It highlights multiple "substantial anomalies" in the DS200, including intermittent screen freezes, system lockups and shutdowns, and failure to log all normal and abnormal system events. For example, the DS200 in some cases failed to log events such as a vote being cast, when its touch-screen is calibrated, and when the system is powered on or off, the EAC said. Though the EAC concluded the problems found prevent the DS200 from meeting federal e-voting system standards, it stopped short of decertifying the system altogether. Source: http://www.computerworld.com/s/article/9223187/E_voting_machine_freezes_misreads_votes_U.S._agency_says?taxonomyId=17

(Florida) **FBI takes over investigation of Florida powder incident.** Three people reported falling ill January 3 after exposure to a suspicious powder in the mail room of the state attorney's office in West Palm Beach, Florida, a city spokesman said. Initial reports indicated the powder was not hazardous, but the investigation will continue, an official with the U.S. Postal

Inspection Service said. Two of the three workers who were sent to a hospital after the exposure complained of headache, nausea, and vomiting, a city spokesman said. The third worker complained of a headache. A firefighter who responded to the incident was also hospitalized with cardiac problems. He was equipped with an air tank, the city spokesman said, and it was unclear whether his symptoms were related to exposure. Other employees were in the mail room when the envelope containing the powder was opened, but they did not complain of any medical problems. A portion of the building evacuated during the scare was reopened after workers sealed off an air duct connecting it to the mail room. The FBI, U.S. postal investigators, and the Palm Beach Sheriff's Office are jointly investigating the case. Source: http://www.cnn.com/2012/01/03/justice/florida-suspicious-powder/index.html?hpt=us_c2

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

Worm slurps 45,000 Facebook passwords. A bank account-raiding worm has started spreading on Facebook, stealing log-in credentials as it moves across the site, security researchers said. Evidence recovered from a command-and-control server used to coordinate the evolving Ramnit worm confirms the malware already stole 45,000 Facebook passwords and associated e-mail addresses. Experts from Seculert, who found the controller node, supplied Facebook with a list of all the stolen credentials found on the server. Most of the victims are from either the United Kingdom or France. Ramnit differs from other worms that use Facebook to spread because it relies on multiple infection techniques, and it only recently extended onto social networks. "Ramnit started as a file infector worm which steals FTP credentials and browser cookies, then added some financial-stealing capabilities, and now recently added Facebook worm capabilities," the CTO at Seculert said. "We suspect that they use the Facebook logins to post on a victim's friends' wall links to malicious Web sites which download Ramnit," he added. Ramnit first appeared in April 2010. By July 2011, variants of the malware accounted for 17.3 percent of all new malicious software infections, according to Symantec. In August 2011, Trusteer reported variants of Ramnit were packing sophisticated banking log-in credential snaffling capabilities — technologies culled from the leak of the source code of the Zeus cybercrime toolkit at around the same time. The new Ramnit configuration was able to bypass two-factor authentication and transaction-signing systems used by financial institutions to protect online banking sessions. The same technology might also be used to bypass two-factor authentication mechanisms to gain remote access to corporate networks, Seculert warns. Source: http://www.theregister.co.uk/2012/01/05/ramnit_social_networking/

Scareware migrates to Android devices, beware of Opera virus scanner. Rogue pieces of software that falsely alert users their devices are infected with malicious elements, requiring victims to pay certain amounts of money to allegedly clean their computers, were spotted to target Android enthusiasts. Up until now, Windows systems were the main target for scareware scams, but Kaspersky Lab researchers found online scam artists are now focusing on smartphones. While searching for some popular mobile apps such as Opera Mini, experts came across several phony Web pages that claim the user's device is infected with malware, requesting access to the phone to provide further details. If the unsuspecting victim accepts,

she is taken to another page that brings up worrying results. The site finds malware in messages, calls, apps, and the storage unit. Unlike the rogue applications that target Windows systems, where the victim is required to provide sensitive data or a certain activation fee, in this case, she is offered a link to activate a "security system" free of charge. Once the alleged system is activated, a trojan identified as SMS.AndroidOS.Scavir is downloaded and installed. After installation is complete, a menu icon similar to the one belonging to Kaspersky applications appears and after making sure it has all the permission it needs, starts sending SMSs to premium rate numbers. The malware targets more than Android users, experts warned. If the phone is detected as running a non-Android operating system, the malicious Web page serves a file called VirusScanner.jar identified as Trojan-SMS.J2ME.Agent.ij. Source: http://news.softpedia.com/news/Beware-of-Opera-Virus-Scanner-Scareware-Migrates-to-Android-Devices-244161.shtml

Stuxnet, Duqu and others created with 'Tilded' platform by the same team. After an extensive analysis of a large number of Stuxnet and Duqu drivers, Kapersky Lab experts concluded the two trojans, along with other pieces of malware, were created by the same team, using a platform called Tilded, created around 2007-2008. They believe Tilded (named so because its authors tend to use file names that start with the symbol *tilde* followed by a letter d (~d)) was utilized to create the two now infamous trojans, which may have been the results of simultaneous projects. The details indicate other spyware modules and programs are based on the same platform. Now, researchers present a precise timeline to show the connection between Duqu and Stuxnet, but also to show the evolution of their drivers from one year to the other. Their studies show a driver called *jmidebs.sys* is the connecting link between *mrxcls.sys* and the drivers later used in Duqu. "The drivers from the still unknown malicious programs cannot be attributed to activity of the Stuxnet and Duqu Trojans. The methods of dissemination of Stuxnet would have brought about a large number of infections with these drivers; and they can't be attributed either to the more targeted Duqu Trojan due to the compilation date," the chief security expert at Kapersky Lab said. "We consider that these drivers were used either in an earlier version of Duqu, or for infection with completely different malicious programs, which moreover have the same platform and, it is likely, a single creator-team." In mid-2010, Tilded went through some changes that may have resulted from the need to better avoid detection by antivirus software, but also because its code could be improved. Source: http://news.softpedia.com/news/Stuxnet-Duqu-and-Others-Created-with-Tilded-Platform-by-the-Same-Team-243874.shtml

National Monuments and Icons

Nothing Significant to Report

Postal and Shipping

Nothing Significant to Report

Public Health

FDA to protect important class of antimicrobial drugs for treating human illness. The U.S. Food and Drug Administration (FDA) issued an order January 4 that prohibits certain uses of the cephalosporin class of antimicrobial drugs in cattle, swine, chickens and turkeys effective April 5, 2012. The FDA is taking this action to preserve the effectiveness of cephalosporin drugs for treating disease in humans. Prohibiting these uses is intended to reduce cephalosporin resistance in bacterial pathogens. Cephalosporins are commonly used in humans to treat pneumonia as well as to treat skin and soft tissue infections. In addition, they are used in the treatment of pelvic inflammatory disease, diabetic foot infections, and urinary tract infections. In its order, the FDA is prohibiting "extralabel" or unapproved uses of cephalosporins in cattle, swine, chickens and turkeys, the so-called major species of food-producing animals. Specifically, the prohibited uses include: using cephalosporin drugs at unapproved dose levels, frequencies, durations, or routes of administration; using cephalosporin drugs in cattle, swine, chickens or turkeys that are not approved for use in that species (e.g., cephalosporin drugs intended for humans or companion animals); using cephalosporin drugs for disease prevention. Source: http://www.fda.gov/NewsEvents/Newsroom/PressAnnouncements/ucm285704.htm

Transportation

Cracked rails from fast chill cause widespread delays on DC Metro system. Sub-freezing temperatures caused rush-hour delays on four of Washington Metropolitan Area Transit Authority's (Metro) five lines January 4, cracking sections of rail along two stretches of track and turning an already cold commute into a frigid marathon for some riders in Washington, D.C., Maryland, and Virginia. Temperatures in the region went from 60 degrees January 1 to the 40s January 2 and then dropped to 17 degrees by January 4, according to the National Weather Service. That caused a shock to the steel rails on Metro's tracks, said Metro's chief spokesman. On the Yellow Line, a 4-inch gap opened in a rail along the bridge across the Potomac River, he said, and a quarter-inch gap was found in a rail on the Red Line near the Takoma station. It can be unsafe to run trains over cracked rail lines, so rail service had to be suspended, and inbound and outbound trains shared a single track on both the Yellow and Red lines, the spokesman said. A nearly 40-foot piece of rail was replaced on the Yellow Line after rush hour, he said. The Red Line crack was temporarily bridged with a "splice bar" that held the pieces together so trains could use that section of track. By 1 p.m., a piece of 40-foot rail went into place on the Red Line to permanently replace the cracked rail. On January 3, in Long Island, New York, broken rail lines due to the cold weather caused 30-minute delays, said a spokesman for the Long Island Rail Road. A spokesman for the Southeastern Pennsylvania Transportation Authority said his transit system has not had cracked-rail problems, but noted sudden changes in temperatures can cause other issues. The change in weather the week of January 2 caused problems with the rail car doors in Philadelphia, which tend to stick when the temperature swings, he said. Source: http://www.washingtonpost.com/local/commuting/cracked-rails-from-fast-chill-cause-widespread-delays-on-dc-metro-system/2012/01/04/gIQAKKuXbP_story.html

Obama signs pipeline safety, airport security laws. The U.S. President signed a bill to toughen oil and gas pipeline regulations and another to ease airport security procedures for members of the military on official travel. He signed the legislation January 3 as part of a post-holiday, back-to-business day that included approval of several other measures approved by Congress late in 2011. The pipeline law aims to close gaps in federal safety regulations made apparent by a fatal gas pipeline break near San Francisco in 2010. The airport security law will allow expedited screening for service members and accompanying family. Military travelers would have to be in uniform and would have to present their orders to benefit from the faster screening process. Source: http://abclocal.go.com/wabc/story?section=news/politics&id=8489903

Water and Dams

(Missouri) **Corps to get $800 million for flood repair.** The Mississippi Valley Division of the U.S. Army Corps of Engineers will receive more than $800 million for repair funds under the Disaster Relief Appropriations Act signed by the U.S. President, December 23. The Corps received $1.7 billion total. The agency intentionally breached a levee in the Birds Point-New Madrid Floodway in May to reduce pressure on a swollen Mississippi River in Mississippi County. The levee breach flooded more than 130,000 acres of farmland and homes. According to the Corps, the Mississippi River and Tributaries System prevented more than $120 billion in damages during the flood in 2011, the largest recorded flood in the river's history. Engineers estimate repair costs for currently documented damages in the Mississippi Valley region alone are close to $1 billion and estimate it will take years to restore the system to its pre-flood conditions. Source: http://www.kfvs12.com/story/16411428/corps-to-get-800-million-for-flood-repair

Billions needed to upgrade America's leaky water infrastructure. At a U.S. Senate hearing in December, a committee was told it will take $335 billion to resurrect water systems and $300 billion to fix sewer systems in the nation. The water pipes in Washington D.C. are being replaced at an average of 11 miles a year. At that rate, replacing them all will take more than 100 years. Officials said there is no money to do it any faster, however, the District's pipes are being replaced twice as fast as the average in other major water systems in America. About $9.4 billion more per year is needed for water and sewer work between now and 2020, according to a study released in December by the American Society of Civil Engineers. Without that, many Americans should prepare for regular disruption of water service and a jump in contamination caused by sewage bacteria, the study said. Nationwide, an estimated 1.7 trillion gallons of water leaks from pipes each year before it can be put to use. About 900 billion gallons of raw sewage flows into waterways. Source: http://www.washingtonpost.com/local/billions-needed-to-upgrade-americas-leaky-water-infrastructure/2011/12/22/gIQAdsE0WP_story.html

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: North Dakota State and Local Intelligence Center: 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov; Fax: 701-328-8175 State Radio: 800-472-2121; Bureau of Criminal Investigation (BCI): 701-328-5500; North Dakota Highway Patrol: 701-328-2455; US Attorney's Office Intel Analyst: 701-297-7400; Bismarck FBI: 701-223-4875; Fargo FBI: 701-232-7241.

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, 701-328-8168